IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

GEORGE ANIBOWEI	§	
	§	
Plaintiff	§	**Civ. Act. No.: 3:16-CV-3495-D**
	§	
v.	§	
	§	**PLAINTIFF'S OPPOSITION**
	§	**TO DEFENDANTS' MOTION**
	§	**TO DISMISS**
LORETTA LYNCH, *et al.*	§	
	§	
Defendants	§	
	§	

PLAINTIFF'S OPPOSITION TO
DEFENDANTS' MOTION TO DISMISS
PLAINTIFF'S FIRST AMENDED COMPLAINT

George Anibowei
Texas Bar No. 24036142
The Law Office of George Anibowei, P.C.
6060 N. Central Expressway, Ste. 560
Dallas, Texas 75206
Telephone No: (214) 800-3463
Facsimile No: (214) 800-3464
Email: ganibowe@yahoo.com
ATTORNEY FOR PLAINTIFF,
GEORGE ANIBOWEI

Table of Contents

Table of Authorities

Cases

Statutes and Rules

Other Authorities

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

GEORGE ANIBOWEI	**§**
	§
Plaintiff	**§ Civ. Act. No.: 3:16-CV-3495-D**
	§
v.	**§**
	§ PLAINTIFF'S OPPOSITION
	§ TO DEFENDANTS' MOTION
	§ TO DISMISS PLAINTIFF'S
LORETTA LYNCH, *et al.*	**§ FIRST AMENDED COMPLAINT**
	§
Defendants	**§**
	§

PLAINTIFF'S OPPOSITION TO
DEFENDANTS' MOTION TO DISMISS
PLAINTIFF'S FIRST AMENDED COMPLAINT

---

1. INTRODUCTION

The question in this case is whether the government can, without any suspicion, take an American's electronic devices from him at the border in order to make copies, retain the copied information indefinitely, examine and analyze the information, and share that information with other parts of the federal government and potentially with foreign governments as well.

Significantly, the government does not contest that this is what happened to Plaintiff George Anibowei when he crossed the border on his way home from vacation on October 10, 2016 and on February 27. 2017. Nonetheless, the government asks this Court to dismiss this case, arguing that neither the Fourth Amendment's prohibition on unreasonable searches and

seizures nor the First Amendment's protections for expressive records and association pose a bar to these actions because its power to search electronic devices is without limit and effectively beyond judicial review. Apparently, the government sees no difference between going through someone's most private papers and examining their shoes and contact lens solution, and asserts it is free to take people's property from them at the border and hold onto it for weeks, months, or even years, if that is how long, in its view, it would take to conduct a search. Additionally, the government also seeks to dismiss this case on the ground that Plaintiff has no legal standing to bring the instant action.

This Court should hold that Plaintiff has standing to bring the instant action. Additionally, the Court should also hold that Plaintiff stated a claim upon which relief can be granted because the government violated his Fourth and First Amendment rights by seizing, copying and dissemination of the information on his electronic devices.

2. BACKGROUND

Plaintiff George Anibowei is a United States Citizen. Plaintiff is a Texas licensed attorney, who is engaged in active and substantial practice of law with offices in Dallas, Texas. Plaintiff was licensed in Texas in 2002 and his Texas Bar Number is: 24036142. Although licensed in the State of Texas in 2002, Plaintiff has been an attorney since 1992, having been licensed in Nigeria before immigrating to the United States. Plaintiff is a frequent international traveler.

On October 10, 2016, after a short vacation in Canada, Plaintiff arrived at the Dallas/Fort Worth International Airport on board American Airlines Flight No. 2609. Upon arrival at the gate and as passengers were getting ready to disembark, the airline crew

directed all passengers to return to their respective seats as officers of DHS were at the gate to remove a passenger and that it was important they did so in an orderly manner. Almost immediately all passengers including the Plaintiff returned to their assigned seats, one of the crew members walked up to the Plaintiff's seat and requested some identification. As soon as Plaintiff tendered his passport, he was informed that the CBP officers were actually at the gate for the Plaintiff. Plaintiff was then instructed to pick up his hand luggage and accompany the crewmember to the gate of the aircraft. The Plaintiff readily complied with the instruction and followed the crewmember to the gate.

Upon exiting the Plane, Plaintiff was accosted by armed officers of the CBP who stated that they were with the Department of Homeland Security (DHS) and requested that the Plaintiff accompany them. Despite repeated requests, the two agents did not explain the reason or the authority for detaining Plaintiff. Instead, they ordered the Plaintiff to place his cell phone in his pocket for "officer safety" and proceeded to escort the Plaintiff like a common criminal through at least three terminals before arriving at their final destination, which is an interrogation room in Terminal D of the Dallas/Fort Worth International Airport.

At the interrogation room, the agents ordered the Plaintiff to empty and place all the content in his pocket on a table. The Plaintiff placed all the contents of his pocket on the table as ordered. Thereafter, one of the agents took Plaintiff's cell phone and directed him to be seated and wait. When the agent returned a short time later, she was no longer in possession of Plaintiff's cellular phone. When Plaintiff asked for his cell phone, he was informed that his cell phone was being detained for "copying and examination". Plaintiff was not asked for his consent and was not presented with a search warrant. Nor was he provided with any explanation of the purpose of the seizure, detention and copying. As authority for taking his

cell phone for copying and examination, he was simply handed a two paged document entitled: Inspection of Electronic Device, copy of which is herewith attached to Plaintiff's Complaint.

Thereafter, the agents continued to detain the Plaintiff and questioned the Plaintiff for approximately two hours. They questioned Plaintiff regarding his background, personal life and purpose of his trip to Canada. Significantly, Plaintiff was asked no questions relating to border control, customs, trade, immigration, or terrorism, and at no point did the agents suggest that plaintiff had broken the law or that his cell phone contained any illegal material. Plaintiff answered their questions truthfully and to the best of his ability.

When Plaintiff was finally allowed to leave, they returned his cell Phone and informed the Plaintiff that its contents have been copied for examination. However, they did not indicate what information had been copied from his cell phone, what agencies or individuals would have access to any copies made, and whether any such copies would ultimately be destroyed or stored.

Subsequent to the filing of this lawsuit and more specifically, on February 12, 2017, Plaintiff embarked on an international travel to Nigeria. On February 27, 2017, Plaintiff arrived at the Dallas/Fort Worth International airport on board Lufthansa Flight No. 438. While going through the US Customs and Border Protection formalities, Plaintiff was yet again referred for secondary inspection. During the secondary inspection, Plaintiff was again detained and questioned by agents of CBP with his cell phone, luggage and carry-on bag subjected to very thorough and rigorous search, much to the detriment, inconvenience, harassment and humiliation of Plaintiff. While undergoing secondary inspection, the CBP agent ordered the Plaintiff to empty and place all the content in his pocket on a table. As

ordered, the Plaintiff complied and placed all the contents of his pocket, including his cell phone, on the table. Thereafter, the agent painstakingly subjected Plaintiff's cell phone to rigorous examination and went through Plaintiff's text messages and emails. Meanwhile, Plaintiff's cell phone contained private and sensitive materials which he did not intend to expose to view by others without his consent. The private and sensitive materials included personal and private information as well as confidential and privileged information concerning his work on behalf of his clients, which he chose to record or store in his cell phone. As in the past, Plaintiff was not asked for his consent and was not presented with a search warrant. Nor was he provided with any explanation of the purpose of the painstaking examination of his cell phone. Thereafter, the agents continued to detain the Plaintiff and questioned the Plaintiff for approximately three hours. Again is in the past, they questioned Plaintiff regarding his background, personal life and purpose of his trip to Nigeria. Significantly, Plaintiff was never asked any questions relating to border control, customs, trade, immigration, or terrorism, and at no point did the agents suggest that Plaintiff had broken the law or that his cell phone contained any illegal material.

3. LEGAL STANDARD

The Supreme Court has clarified the law with respect to what a Plaintiff must plead in order to survive a Rule 12(b)(6) motion. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). The Court stated that "a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Id. at 1964–65 (citations and quotation marks omitted). Additionally, the Court emphasized that even though a complaint need not contain "detailed" factual allegations, its "[f]actual allegations must be enough to

raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true." *Id*. (internal citation and quotation marks omitted). In so holding, the Court disavowed the oft-quoted Rule 12(b)(6) standard of *Conley v. Gibson*, 355 U.S. 41, 45–46, 78 S. Ct. 99, 2 L.Ed.2d 80 (1957) (recognizing "the accepted rule that a complaint should not be dismissed for failure to state a claim unless it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief"), characterizing that rule as one "best forgotten as an incomplete, negative gloss on an accepted pleading standard." *Twombly*, 550 U.S. at 563.

4. ARGUMENT

The legal question in this case is whether the government can, without any suspicion, take an American's electronic devices from him at the border in order to make copies, retain the copied information indefinitely, examine and analyze the information, and share that information with other parts of the federal government and potentially with foreign governments as well, without the citizen's consent, and without providing any explanation of the reasons behind this unlawful acts.

At the outset, it is significant and very pertinent to note that the government does not contest the allegations contained in the Plaintiff's Complaint. Instead, the government asks this Court to dismiss this case, because neither the Fourth Amendment's prohibition on unreasonable searches and seizures nor the First Amendment's protections for expressive records and association pose a bar to these actions arguing that, first, the Plaintiff "*lacks standing to obtain the equitable relief he seeks, because the fact that Anibowei was exposed to allegedly illegal conduct in the past is not sufficient to entitle him to litigate any claim in*

federal court absent some showing that the allegedly illegal act will be repeated against him in the future," and secondly, because "*Anibowei has failed to state a claim upon which relief can be granted because neither the Fourth Amendment nor the First Amendment requires a showing of reasonable suspicion before an electronic device can be searched at the border".* (Defendants' Motion to Dismiss Plaintiff's First Amended Complaint– page 1)

I. Plaintiff has Legal Standing

The law of standing has its roots in Article III's case and controversy requirement. *See Summers v. Earth Island Institute*, 555 U.S. 488, 492-93 (2009); *DaimlerChrysler Corporation v. Cuno*, 547 U.S. 332, 340-41 (2006). The U.S. Supreme Court has established a three-part test for standing. The "irreducible constitutional minimum of standing" requires the plaintiff to establish:

First, an "injury in fact"—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) "actual or imminent," not "conjectural" or "hypothetical." Second, there must be a causal connection between the injury and the conduct complained of - the injury has to be "fairly ... trace[able] to the challenged action of the defendant, and not ... th[e] result [of] the independent action of some third party not before the court." Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision." See *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *see also Summers*, 555 U.S. at 493.

Inherent in the constitutional limitation of judicial power on cases and controversies is the requirement of "concrete adverseness" between the parties to a lawsuit. The Supreme Court requires that plaintiff establish that the challenged conduct caused or threatens to cause them an injury in fact to judicially cognizable interests. By establishing that they personally

suffered injury, plaintiffs demonstrate that they are sufficiently associated with the controversy to be permitted to litigate it. The question of injury raises two questions – (1) what kinds of injuries count for purposes of standing; and, (2) how certain the injury must be if it has not yet occurred.

The Supreme Court has held that, to satisfy the injury in fact requirement, a party seeking to invoke the jurisdiction of a federal court must show three things: (1) "an invasion of a legally protected interest," (2) that is "concrete and particularized," (3) "actual or imminent, not conjectural or hypothetical." See *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

A particularized injury "must affect the plaintiff in a personal and individual way." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560 n.1).

In the present case, the violation of the Plaintiff's constitutional rights did occur prior to the Plaintiff filing the federal lawsuit in this case; and, significantly has again occurred even after the Plaintiff filed this lawsuit. (See Doc. 8, ¶ 38) The injury to the Plaintiff is ongoing, and because the Plaintiff is a frequent flyer, as stated in his complaint, there is a real and immediate threat of repeated injury in the future with no end in sight. Therefore, the Plaintiff has clearly met the conditions set by the Supreme Court in *Lujan v. Defenders of Wildlife* (*Supra*). Plaintiff's case is not based on speculation. Rather it is based on actual injury, which occurred prior to and subsequent to the filing of Plaintiff's lawsuit.

The Plaintiff therefore respectfully request that this honorable Court must hold that Plaintiff has the requisite legal standing to bring this suit. This is especially so considering that the government has not denied the wrongdoing to the Plaintiff. It has only claimed

unquestionable right to violate Plaintiff's constitutional rights. As Plaintiff's First Amended Complaint shows, the fact that the Plaintiff is already seeking the protection of the court to enforce his constitutionally protected rights did not deter the government from continuing to violate the Plaintiff's rights for no apparent reason whatsoever by repeating the illegal conduct complained of in this case even after the filing of this law suit. Basically, the Plaintiff has demonstrated a continuing harm or at the very least, a real and immediate threat of repeated injury in the future. Therefore, this court must hold that Plaintiff has legal standing to bring the instant action.

II. The Court must accept the non-conclusory factual allegations in the complaint as true.

To survive a motion to dismiss, a complaint "must 'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests,' and allege 'a plausible entitlement to relief.'' *Decotiis v. Whittemore*, 635 F.3d 22, 29 (1st Cir. 2011) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 559 (2007)). The Court accepts non-conclusory factual allegations in the complaint as true, *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 12 (1st Cir. 2011), and "draw[s] all reasonable inferences in favor of the plaintiff." *Gargano v. Liberty Int'l Underwriters, Inc.*, 572 F.3d 45, 48 (1st Cir. 2009). "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 545 (internal quotation marks and citations omitted). However, considering a motion to dismiss is "neither the time nor the place to resolve the factual disputes between the parties", whether [the plaintiff] can prove what he has alleged is not the issue. At this stage of the proceeding, we must take the complaint's factual allegations as true,

as long as they paint "a plausible picture." *See Haley v. City of Boston*, 657 F.3d 39, 52 (1st Cir. 2011).

Considering that the court must take the complaint's factual allegations as true, it is necessary to examine Plaintiff's Factual Allegations, which must be taken as true.

On October 10, 2016, after a short vacation in Canada, Plaintiff arrived at the Dallas/Fort Worth International Airport on board American Airlines Flight No. 2609. Upon arrival at the gate and as passengers were getting ready to disembark, the airline crew directed all passengers to return to their respective seats as officers of DHS were at the gate to remove a passenger and that it was important they did so in an orderly manner. Almost immediately all passengers including the Plaintiff returned to their assigned seats, one of the crewmembers walked up to the Plaintiff's seat and requested some identification. As soon as Plaintiff tendered his passport, he was informed that the CBP officers were actually at the gate for the Plaintiff. Plaintiff was then instructed to pick up his hand luggage and accompany the crewmember to the gate of the aircraft. The Plaintiff readily complied with the instruction and followed the crewmember to the gate. Upon exiting the plane, Plaintiff was accosted by armed officers of the CBP who stated that they were with the Department of Homeland Security and requested that the Plaintiff accompany them. Despite repeated requests, the two agents did not explain the reason or the authority for detaining Plaintiff. Instead, they ordered the Plaintiff to place his cell phone in his pocket for "officer safety" and proceeded to escort the Plaintiff like a common criminal through at least three terminals before arriving at their final destination, which is an interrogation room in Terminal D of the Dallas/Fort Worth International Airport.

At the interrogation room, the agents ordered the Plaintiff to empty and place all the content in his pocket on a table. The Plaintiff placed all the contents of his pocket on the table

as ordered. Thereafter, one of the agents took Plaintiff's cell phone and directed him to be seated and wait. When the agent returned a short time later, she was no longer in possession of Plaintiff's cellular phone. When Plaintiff asked for his cell phone, he was informed that his cell phone was being detained for "copying and examination". Plaintiff was not asked for his consent and was not presented with a search warrant. Nor was he provided with any explanation of the purpose of the detention, copying and examination. As authority for taking his cell phone for examination and copying, he was simply handed a two paged document entitled: Inspection of Electronic Device, copy of which is attached to Plaintiff's First Amended Complaint and incorporated herein by reference.

Thereafter, the agents continued to detain the Plaintiff and questioned the Plaintiff for approximately two hours. They questioned Plaintiff regarding his background, personal life and purpose of his trip to Canada. Significantly, Plaintiff was asked no questions relating to border control, customs, trade, immigration, or terrorism, and at no point did the agents suggest that plaintiff had broken the law or that his cell phone contained any illegal material. Plaintiff answered their questions truthfully and to the best of his ability. When Plaintiff was finally allowed to leave, they returned his cell Phone and informed the Plaintiff that its contents have been copied for examination. However, they did not indicate what information had been copied from his cell phone, what agencies or individuals would have access to any copies made, and whether any such copies would ultimately be destroyed or stored. Significantly, the government has not disputed Plaintiff's Factual allegations.

As Plaintiff's First Amended Complaint shows, subsequent to the filing of this lawsuit and more specifically, on February 12, 2017, Plaintiff embarked on an international travel to Nigeria. On February 27, 2017, Plaintiff arrived at the Dallas/Fort Worth

International Airport on board Lufthansa Flight No. 438. While going through the US Customs and Border Protection formalities, Plaintiff was yet again referred for secondary inspection. During the secondary inspection, Plaintiff was again detained and questioned by agents of CBP with his cell phone, luggage and carry-on bag subjected to very thorough and rigorous search, much to the detriment, inconvenience, harassment and humiliation of Plaintiff. While undergoing secondary inspection, the CBP agent ordered the Plaintiff to empty and place all the content in his pocket on a table. As ordered, the Plaintiff complied and placed all the contents of his pocket, including his cell phone, on the table. Thereafter, the agent painstakingly subjected Plaintiff's cell phone to rigorous examination and went through Plaintiff's text messages and emails. Meanwhile, Plaintiff's cell phone contained private and sensitive materials, which he did not intend to expose to view by others without his consent. The private and sensitive materials included personal and private information as well as confidential and privileged information concerning his work on behalf of his clients which he chose to record or store in his cell phone. As in the past, Plaintiff was not asked for his consent and was not presented with a search warrant. Nor was he provided with any explanation of the purpose of the painstaking examination of his cell phone. Thereafter, the agents continued to detain the Plaintiff and questioned the Plaintiff for approximately three hours. Again, as in the past, they questioned Plaintiff regarding his background, personal life and purpose of his trip to Nigeria. Significantly, Plaintiff was never asked any questions relating to border control, customs, trade, immigration, or terrorism, and at no point did the agents suggest that Plaintiff had broken the law or that his cell phone contained any illegal material.

Accepting the non-conclusory factual allegations in the complaint as true, the

Plaintiff has clearly stated a claim upon which relief could be granted and the Court must so hold.

III. Some level of suspicion is Required for seizing, searching and copying US citizen Traveler's electronic devices at the Border

The Fourth Amendment guarantees "the right of the people to be secure in their persons…. and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . ." U.S. CONST. amend. IV. However, any analysis of a border search must begin from the proposition that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Therefore, it is well-established "[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). "Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . ." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). But even at the border, the Fourth Amendment continues to protect against *unreasonable* searches and seizures; the only difference is that, at the border, *routine* searches become reasonable because the interest of the Government is far stronger and the reasonable expectation of privacy of an individual seeking entry is considerably weaker. *See Carroll v. United States*, 267 U.S. 132, 154 (1925) ("Travelers may be stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may lawfully be brought in.").

But cf. United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (holding that the Fourth Amendment does not apply to non-citizens searched or seized outside of the United States). However, when a search stretches beyond the *routine*, it must rest on reasonable, particularized suspicion, *Montoya de Hernandez*, 473 U.S. at 541, which is significantly less demanding than the showing of probable cause required to secure a warrant for a domestic search, *see* U.S. Const. amend. IV. While the Supreme Court has not addressed the issue often, it has laid out the broad strokes of what constitutes a routine, versus a nonroutine, search.

As indicated, the Supreme Court has recognized certain limitations to the border search power to conduct routine searches without some level of suspicion. For instance, customs officials need some level of suspicion to conduct "highly intrusive searches" implicating the "dignity and privacy interests" of a person such as body cavity or strip searches. *See Flores-Montano*, 541 U.S. at 152 (holding that the removal, disassembly and reassembly of a vehicle's fuel tank at the border did not require particularized suspicion). Similarly, the Supreme Court has described strip, body cavity, or involuntary x-ray searches as "nonroutine border searches" but expressly declined to suggest "what level of suspicion, if any, is required" for these searches. *Montoya de Hernandez*, 473 U.S. at 541 n. 4. Furthermore, in addition to the "highly intrusive searches of the person," *Flores-Montano*, 541 U.S. at 152, the Supreme Court has left open the question "whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it was carried out," *Id.* at 155, n. 2 (quoting Ramsey, 431 U.S. at 618 n.13), but has not defined the precise contours of a search carried out in such a manner. Besides, the Supreme Court has also suggested the possibility that "some searches of property are so destructive as

to require" some level of suspicion. *Flores-Montano*, 541 U.S. at 155-56.

The Plaintiff contends that the seizure, search, copying and examination of his cell phone was highly intrusive implicating his dignity and privacy interests given the personal nature and quality of information stored on the device and because the search was conducted in a particularly offensive manner and such "non-routine" search would only have comported with the Fourth Amendment if the agents had some level of suspicion.

The Defendants do not argue that the agents had reasonable suspicion or any reason to conduct the search and seizure but rather rely on the argument that none was required. More specifically, Defendants wrongly contend that they have unreviewable discretion to search the private information on individual's electronic device and to seize the device for as long as they like. There are three reasons why a search of a private electronic device triggers a reasonable suspicion requirement: (1) It is non-routine (2) It is particularly offensive (3) It imposes a serious burden on First Amendment activity.

Electronic devices are not like socks or contact lens solution; they are repositories of our intimate and private personal information, not just those needed for one trip but a complete archive of our thoughts for many years. The doctrines Defendants lean on, such as the closed container doctrine, were developed in a different time and in another context. In addressing this issue, it is appropriate to consider the Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014). Although that decision does not specifically address a search of a cell phone conducted at the border, the Supreme Court in *Riley* made clear that cell phones are categorically different from other personal effects, such as containers. 134 S. Ct. 2484-85, 2489-91. Indeed, the Supreme Court in *Riley* noted that the suggestion that a data search of a cell phone is "materially indistinguishable" from searches of physical items was

"like saying a ride on horseback is materially indistinguishable from a flight to the moon" because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 2488-89.

At this stage, it is perhaps pertinent and very important to understand what takes place during a forensic search of a computer or an electronic device such as a smart cell phone, and what distinguishes it from what may usefully be regarded as a "conventional" or routine search of a computer or digital device. Though every search is different, a forensic search has certain hallmarks by which it can be identified. First, "the computer forensics process always begins with the creation of a perfect 'bitstream' copy or 'image' of the original storage device saved as a 'read only' file." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 540 (2005). Then, a computer forensics expert will use specialized software to comb through the data, often over the course of days, weeks, or even months, *id.* at 537–38, searching the full contents of the imaged hard drive, examining the properties of individual files, and probing the drive's unallocated "slack space" to reveal deleted files, *id.* at 542–43. Although directed by a forensic examiner, an integral part of a forensic examination is the use of technology-assisted search methodology, where the computer searches vast amounts of data that would exceed the capacity of a human reviewer to examine in any reasonable amount of time. The techniques used during a forensic search can be distinguished from a conventional computer search, in which a Customs officer may operate or search an electronic device in much the same way that a typical user would use it.

Basically, a conventional computer search can be deeply probing and, much like any search of personal effects at the border, has the potential to be invasive. Yet these

concerns do not bring a conventional computer search outside of the broad authority granted under the border search doctrine any more than a suitcase is immunized from search because it may contain a personal diary. Despite the vast amounts of data available in an electronic device, a conventional search is limited by the amount of time one Customs officer has to devote to reviewing the contents of digital evidence at the border while its owner awaits the outcome of the search. Even if that review may take a matter of hours, the amount of data searched will be a mere fraction of what is on the device, given the storage capacity of modern electronic devices. And in any event, though such a search may last hours, it will not last days. There is only so much time that a Customs officer has to devote to the border search of a computer. No matter how thorough or highly motivated the agent is, a manual search of a computer or digital device will never result in the human visualization of more than a fraction of the content of the device.

In contrast, a forensic examination of a computer or other electronic device using sophisticated technology-assisted search methodologies can exceed vastly the capacity of a human searching and viewing files. Moreover, this type of search exposes a class of data that raises novel privacy concerns, including files that a user had marked as "deleted"[1] and location data that may provide information about activities in the home and away from the border. For this reason, a forensic search of an electronic device differs significantly from a conventional search not merely in degree, but in kind. More specifically, an individual's privacy interest in the information contained on his cell phone is much greater than an

[1] The mere act of marking a file as "deleted" does not actually delete it from a computer; rather, it merely removes references to the file from the computer's Master File Table, which marks the data clusters where the file is located as available for future use. The file itself will remain until those clusters actually are overwritten or are "zeroed out" so as to remove the file itself from the computer. Kerr, *supra*, at 542–43.

individual's privacy interest in the contents of his luggage or other personal effects. Indeed, a cell phone cannot fairly be compared to an ordinary container that might be searched at the border because as the Supreme Court in *Riley* made clear, "[a] phone not only contains in digital form many sensitive records previously found in the home," but also "a broad array of private information never found in a home in any form - unless the phone is [in the home]." *Id.* at 2491. As one court has noted, "[i]t is difficult to conceive of a property search more invasive or intrusive" than a sophisticated, digital search of a cell phone because such a search is "essentially a body cavity search" of the cell phone. *See United States v. Saboonchi*, 990 F.Supp.2d 536 at 569 (D. Md.2014) (holding that forensic digital searches are nonroutine border searches, and therefore reasonable suspicion is required, on the ground that "[i]t is difficult to conceive of a property search more invasive or intrusive than a forensic computer search - it essentially is a body cavity search of a computer). Thus, even at the border, an individual has a significant privacy interest in the digital contents of his cell phone.[2] Accordingly, a forensic search of an electronic device seized at the border cannot be performed absent reasonable, articulable suspicion because such a search is clearly non-routine. This conclusion is compelled in light of the fact that the Supreme Court has made clear that under the border search exception, only routine border searches are wholly immune

---

[2] *See* United States v. Cotterman, 709 F.3d 952, 956–57 (9th Cir. 2013) (en banc), where the Ninth Circuit required a showing of reasonable suspicion to justify the government's detention and shipping of the defendant's laptop computer 170 miles from the border to perform a "comprehensive forensic evaluation" at a later date, which search was capable of restoring deleted material and retrieving images viewed on web sites. The Ninth Circuit's reasoning was essentially that these actions were so intrusive as to require reasonable suspicion, see id. at 962–68

from the typical Fourth Amendment requirements, whereas nonroutine border searches must rest on some degree of particularized suspicion. *Montoya de Hernandez,* 473 U.S. at 541, 105 S.Ct. 3304.

IV. The Suspicionless Search of Mr. Anibowei's Electronic Device Violated His Fourth Amendment Rights.

Plaintiff has alleged that Defendants had no reasonable suspicion to search his electronic devices and Defendants do not suggest otherwise. Thus, this Court must accept Plaintiff's assertion that Defendants searched Plaintiff's electronic device without suspicion. Fed. R. Civ. P. 8(b)(6). Clearly, under the circumstances of this case, the Fourth Amendment prohibits the government from searching the contents of Mr. Anibowei's electronic devices at the border absent reasonable suspicion, for three reasons:

(1) Because of their invasive nature, searches of electronic devices are "non-routine" searches that require reasonable suspicion.

(2) Suspicionless electronic device searches are unreasonable because of the "particularly offensive manner" in which they are carried out.

(3) Because electronic device searches involve searches of First Amendment-protected material, the reasonable suspicion standard is the constitutional minimum

(1) The Search of Mr. Anibowei's Electronic Device was Non-Routine

The border is not a Fourth Amendment-free zone. Although the Supreme Court has found that the government has broad powers to conduct searches at the border, *see United States v. Ramsey*, 431 U.S. 606, 616 (1977), it has also recognized that "non-routine" border searches require at least reasonable suspicion of wrongdoing, *Montoya de Hernandez,* 473 U.S. at 541. The First Circuit has held that when deciding whether a search is non-routine, the determining factor is "[t]he degree of invasiveness or intrusiveness." *See United States v. Braks,* 842 F.2d

509, 511 (1st Cir. 1988). There is no question that the uniquely private and vast amount of information stored on electronic devices renders searches of these devices highly invasive.

There is no gainsaying the fact that a forensic search of an electronic device intrudes upon a traveler's dignity and privacy. In this case, the search of Plaintiff's cell phone, which involved the copying of every bit of data contained on the phone's hard drive clearly intrudes upon Plaintiff's dignity and privacy. To suggest otherwise is like suggesting that a strip search does not implicate a significant privacy interest so long as the government does not look between the person's toes.

With each passing day, people conduct and store more of their lives on computers, smart phones, and other electronic devices. These devices are far more than receptacles for private files; they have become a commonplace part of the daily life of the average person. They are constantly used to help people think, learn, communicate, associate with others, and keep track of their own lives and those of their families. *See generally* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 Widener L.J. 667 (2006). A consequence of this new reality is that these devices also maintain a nearly indelible record of everything their users think or search for, what they learn or read, what they say to others, and with whom they associate. Basically, a cell phone such as the Plaintiff's contains an immense amount of disparate personal information. Indeed and as rightly noted by the Supreme Court in *Riley*, a search by the government of such an immense amount of disparate personal information allows the government to pretty much reconstruct "an individual's private life". *Riley*, 134 S. Ct. at 2489

The information stored on Mr. Anibowei's smart phone, for example, spanned a period of years and included emails "sent to and from family members and friends and messages

concerning employment related matters, records of his personal finances, computer programming work in progress, and passwords allowing access to his bank account, his workplace computer, and privileged communications with his clients". Given the nature of information commonly stored on electronic devices, it should come as no surprise that "for most people, their computers are their most private spaces." *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting).

Electronic devices are the gateway to the Internet and all it has to offer, including means of communication such as e-mail, instant messaging, and social networks. As the Sixth Circuit recently noted in holding that individuals have a right to privacy in email:

> "Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted [access to] a subscriber's emails without triggering the machinery of the Fourth Amendment." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

Suspicionless searches of electronic devices that facilitate, record, and store such communications undoubtedly implicate heightened concerns of privacy and dignity that distinguish the devices from other types of property that travelers may carry across the border.

The vast quantity of information contained on electronic devices magnifies the privacy and dignity concerns implicated by a border search. A computer "is akin to a vast warehouse of information," and a typical hard drive sold in 2005 can carry data "roughly equivalent to forty million pages of text - about the amount of information contained in the books on one

floor of a typical academic library." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175 (9th Cir. 2010) ("[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information."). Such a vast quantity and variety of information increases the likelihood that highly personal information will also be searched, seized, or copied. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994). As a consequence, individuals' privacy and dignity interests in the contents of their laptops and similar electronic devices more closely resemble the heightened interests associated with private dwelling areas and should be treated accordingly. *Cf. United States v. Cardona-Sandoval*, 6 F.3d 15, 21-23 (1st Cir. 1993) (distinguishing between an individual's private space and communal public areas of a vessel in analyzing reasonableness of search at sea); *United States v. Whitted*, 541 F.3d 480, 489 (3d Cir. 2008) (requiring suspicion for a border search of a passenger cabin in a vessel); *United States v. Alfonso*, 759 F.2d 728, 738 (9th Cir. 1985) (finding that a border search of the private living quarters on a ship "should require something more than naked suspicion").

The reasonable suspicion standard is not novel. It is a longstanding and familiar standard that border agents already apply in cases of personally invasive searches. Moreover, the vast number of cases finding reasonable suspicion to justify border searches of electronic devices belies Defendants' suggestion that applying the standard would thwart border agents' ability to effectively police the borders. *See, e.g.*, *United States v. Irving*, 452 F.3d 110, 124 (2d Cir. 2006); *United States v. Roberts*, 274 F.3d 1007, 1012 (5th Cir. 2001); *United States v. Bunty*, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008); *United States v. Hampe*, No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007), *aff'd* No. CR-07-3-B- W, 2007 WL

1806671 (D. Me. June 19, 2007); *United States v. Furukawa*, No. 06-145 (DSD/AJB), 2006 WL 3330726, at *2 (D. Minn. Nov. 16, 2006); *cf. Whitted*, 541 F.3d. at 489 ("Reasonable suspicion is not a high standard that will prevent customs officers from detecting drug smugglers at our borders.").

(2) The Search of Mr. Anibowei's Electronic Devices was particularly offensive in Manner

In *Ramsey*, the Supreme Court stated that a border search may be constitutionally objectionable "because of the particularly offensive manner in which it is carried out." 431 U.S. at 618 n.13. Citing to cases in which the Court had limited the extent to which the government could conduct broad-ranging searches or seizures incident to arrest, the Court suggested that the offensiveness of the execution of a search may violate the Constitution. *Id.* Electronic Device searches are similarly offensive in manner.

As described above, electronic devices contain vast quantities of deeply personal and sensitive information. Several federal courts have recognized that because electronic device searches risk devolving into exploratory rummaging through this personal and sensitive information, judicial officers must engage in "greater vigilance . . . in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177 (upholding ex ante limits on the execution of warrants to search electronic devices); *accord United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 958-59 (N.D. Ill. 2004); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998). Although these cases did not involve border searches, they are informed by the very Fourth Amendment concerns about fishing expeditions that the *Ramsey* Court warned might render a border search unreasonable. Therefore, Defendants'

claim of authority to roam through Mr. Anibowei's electronic devices without reasonable suspicion must fail.

(3) The Search of Mr. Anibowei's Electronic Device Burdened his Expressive and Associational interests

Electronic device searches invariably involve examining an extensive amount of expressive and associational material, and the search of Mr. Anibowei's electronic devices was particularly troubling because of the unquestionable burden it places on his Expressive and Associational interests. When a search or seizure burdens First Amendment interests, those interests must be considered in determining whether the search or seizure is reasonable. Because they implicate expressive and associational interests, conducting searches and seizures of electronic devices in the absence of suspicion is unreasonable and violates the Fourth Amendment.

Not all searches and seizures are the same; "[a] seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." *Roaden v. Kentucky*, 413 U.S. 496, 501 (1973). As *Roaden* held, seizures of expressive materials, such as "books and movie films," are "to be distinguished from" seizures of "instruments of a crime" or "contraband" in appraising reasonableness. *Id.* at 502 (quotation marks omitted). Examining reasonableness "in the light of the values of freedom of expression," the Court required police to obtain a warrant to seize expressive materials even though one would not otherwise have been required. *Id.* at 504. Courts have held that associational material is likewise entitled to heightened procedural protections. *See, e.g.*, *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460-61 (1958).

Searches that implicate First Amendment-protected materials therefore require the application of heightened Fourth Amendment requirements, up through and including a

warrant and probable cause, even where those requirements might not otherwise apply. *Roaden* at 501- 04; *see also Maryland v. Macon*, 472 U.S. 463, 468 (1985) ("First Amendment imposes special constraints on searches for and seizures of presumptively protected material."). Relatedly, the Fourth Amendment's procedural protections must be applied with "scrupulous exactitude" when a search implicates expressive materials. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Stanford v. Texas*, 379 U.S. 476, 485 (1965). Because searching electronic devices implicates expressive and associational interests, more procedural protections are required than may typically apply to unprotected materials searched at the border. While these cases did not involve the border, the border is not a Fourth amendment-free zone especially as it affects a United States citizen. The Supreme Court has repeatedly rejected the proposition that the border is a Fourth Amendment-free zone, *see, e.g.*, *Montoya de Hernandez*, 473 U.S. at 537-38, and has suggested that government intrusions that implicate expressive conduct, even at the border, should be policed especially carefully by courts, *see, e.g.*, *Ramsey*, 431 U.S. at 624 (suggesting that "full panoply of Fourth Amendment requirements" might be applicable where government searches implicate expressive rights or threaten to "chill" expressive conduct (citing, *inter alia*, *Roaden* and *Stanford*)).

In sum, searching electronic devices is different than searching ordinary luggage, and Mr. Anibowei did not lose his right to privacy in expressive and associational materials simply because he crossed the border. *Cf. Lamont v. Postmaster Gen.*, 381 U.S. 301, 305 (1965) (holding that restrictions on unfettered delivery of mail from abroad infringed addressees' First Amendment rights).

V. Defendants' Actions violated the First Amendment

Mr. Anibowei's cell phone/electronic device contained private and sensitive materials including personal and private information and information concerning his work on behalf of his clients, most of which are privileged and confidential communications between Attorney and Client that he did not intend to expose to view by others without his consent. Additionally, Mr. Anibowei's cell phone/electronic device also contained his personal e-mail communications covering a period of several years, including messages sent to and from family members and friends, records of his personal finances, passwords allowing access to his bank account, to his workplace computer, and to secure communications websites, and as previously indicated, privileged communications between him as an Attorney and his clients. The seizure, copying and retention of this information and its dissemination to other governments, agencies, private entities, individuals, or the public at large will not only adversely affect the Plaintiff, but may also affect his innocent clients.

Clearly, the government's actions have violated Mr. Anibowei's First Amendment right to association. *Ashcroft v. Iqbal*, 129 S. Ct. 1937 (2009). Meanwhile, the Government seeks outright dismissal of Plaintiff's claims despite the fact that the seizure, copying and dissemination of sensitive and privileged material on his smart phone violates the right of association guaranteed by the First Amendment giving rise to Plaintiff's legal claims. Defendants' position oversimplifies the *Iqbal* standard, and understates the intrusion on Plaintiff's First Amendment rights. Unquestionably, the Plaintiff has alleged sufficient plausible basis for his legal claims in his Complaint. Therefore, the dismissal of Plaintiff's complaint pursuant to Rule 12(b)(6) is inappropriate since the properly pleaded allegations of fact state a facially plausible legal claim. *See Belyea v. Litton Loan Servicing, LLP*, Civ.

Action No. 10-10931-DJC, 2011 WL 2884964, at *1 (D. Mass. July 15, 2011) (citing *Ocasio–Hernández v. Fortuño–Burset*, 640 F.3d 1, 11-12 (1st Cir. 2011)).

Plaintiff has alleged that information was copied from his cell phone and retained by the Defendants and that the information so copied has been disseminated to other government agencies including the "non-DHS Defendants". The complaint alleges that the data that was copied, shared, and retained contained important and sensitive information about the Plaintiff and his family, including privileged and confidential communications between the Plaintiff and his clients. Curiously, the Motion to Dismiss filed by the government does not address the allegation that the information was shared with and retained by other agencies of the federal government. Therefore, that allegation must be taken as true for purposes of Defendants' Rule 12(b)(6) motion.

These allegations fairly meet *Iqbal'*s requirements. Courts have recognized time and again that the harms which Defendants describe as mere "speculation….about what [Plaintiff] thinks may happen" are sufficient to establish a burden on fundamental rights. "[C]ompelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment." *Buckley v. Valeo*, 424 U.S. 1, 64 (1976). This is obviously true in cases where the threat of imminent harm has been shown on the record, *e.g*, *NAACP v. Alabama*, 357 U.S. at 462; *Bates v. City of Little Rock*, 361 U.S. 516, 521-522 (1960), but has been recognized as well where the concern was less extensively supported, *e.g.*, *Shelton v. Tucker*, 364 U.S. 479, 485-86 (1960) ("to compel a teacher to disclose his every associational tie is to impair that teacher's right of free association"), and in cases where there has been no record of retaliation, *see Talley v. California*, 362 U.S. 60, 65 (1960) (blanket prohibition of anonymous handbills invalidated because fear of reprisal might deter discussion of public

matters); *Pollard v. Roberts*, 283 F. Supp. 248, 258 (E.D. Ark. 1968) (3 judge court), *aff'd per curiam* 393 U.S. 14 (1968) (no evidence that any individuals had been subjected to reprisals on account of support for Republican candidates); *Johnson v. Wash. Times Corp*., 208 F.R.D. 16, 17-18 (D.D.C. 2002) (general claim of bigotry against members of a "controversial" church sufficient)

The Second Circuit's opinion in *Tabbaa v. Chertoff*, 509 F.3d 89 (2 Cir. 2007), although ultimately resolved in favor the government, supports Plaintiff's position here. The court found that an extended border stop of individuals returning from an Islamic conference in Canada, involving detention for several hours, questioning, photographing, and fingerprinting, while not exceeding the bounds of a routine search, was sufficient to implicate the protections of the First Amendment because "the prospect of being singled out for such extensive processing could reasonably deter others from associating at similar conferences." *Id.* at 102.

The First Amendment claim was rejected only because the government had presented sufficient evidence to establish that it had a compelling interest in preventing terrorists who had attended the conference from entering the United States. *Id*. at 103. Here, however, the government has made no claim that the seizure and retention of information from the Plaintiff's electronic device was justified for any reason other than the fact that it took place at the border.

Clearly, the government's search of Plaintiff's electronic devices burdened his First Amendment rights because it forced him to reveal to the government his thoughts where those thoughts had previously been shielded from observation. Yet, the government has failed to put forth any reasons it had to justify a search of Mr. Anibowei's electronic devices, other than a

vague and generalized interest in border security. This interest is not sufficient to satisfy the heightened scrutiny that applies to searches of expressive records.

Significantly, to support their argument that there is no First Amendment exception to the border-search doctrine, the Defendant's relied heavily on *United States v. Ickes,* 393 F.3d 501 (4th Cir.2005) – a fourth circuit decision, which declined to carve out a First Amendment exception for the search of electronic device simply because the device contained expressive materials. However, this reliance is clearly misplaced because the facts surrounding the seizure in *Ickes* are different in significant respects than those alleged in the Complaint in this case. In *Ickes,* the Fourth Circuit addressed a digital border search of an electronic device. There, as part of a routine border inspection, the government discovered, *inter alia,* a video camera with "a tape of a tennis match which focused excessively on a young boy" and "several albums containing photographs of provocatively-posed prepubescent boys, most nude or semi-nude." *Id.* at 502, 503. The government agents arrested the defendant, and continued to search the van, discovering a computer and approximately seventy-five disks. *Id.* After seizing the computer and disks, government agents searched the contents of these electronic devices and found that they contained child pornography. *Id.* Specifically, government agents manually investigated the contents of the computer and the disks by accessing their content in the same way a typical user would do so; the government did not conduct a sophisticated forensic analysis of the contents of the computer and the disks. *Id.* The Fourth Circuit in *Ickes* held that the manual digital border search of the computer and disks was routine, and therefore did not require any level of suspicion. *Id.* at 505-06. The Fourth Circuit reached this conclusion by comparing computer files to the physical contents of any other "cargo" subject to a routine search and inspection at the border. *Id.* at 504. In this regard, the Fourth Circuit

held that a manual review of electronic files contained on a computer is no different than a manual review of papers contained in luggage, a classic example of a routine border search. *Id.* at 505-06. Besides and importantly, in *Ickes,* the agents did not inspect the contents of the defendant's computer until after they had discovered marijuana paraphernalia, photo albums of child pornography, a disturbing video focused on a young ball boy, and an outstanding warrant for the defendant's arrest. 393 F.3d at 507. In holding that Defendant had failed to state a First Amendment claim, the Fourth Circuit noted that "[a]s a practical matter, computer searches are most likely to occur where, as here, the traveler's conduct or the presence of other items in his possession suggest the need to search further." *Id*. In contrast to the searches and seizures at issue in I*ckes,* here, there is nothing in Plaintiff's conduct or the presence of other items in his possession to suggest the need to search further by copying the entire data of information from his cell phone for subsequent examination and dissemination to other government agencies.

Although *Ickes* clearly stands for the proposition that a manual digital search of an electronic device is a routine border search, that decision does not address whether more sophisticated forensic searches such as copying and subsequent examination of the entire data of electronic devices at the border may properly be classified as routine border searches. In this regard, it is important to note that one district court in the fourth circuit has had cause to address whether a forensic search of a cell phone is a routine border search. *See United States v. Saboonchi,* 990 F.Supp.2d 536 (D. Md.2014).

In *Saboonchi,* border agents confiscated two cell phones and a flash drive after stopping the defendant and his wife at the border. *Id.* at 539. The border agents searched both cell phones by creating "a perfect bitstream copy" - a complete copy – "of the original storage

device" and then using "specialized software to comb through the data ... searching the full contents of the [copied] hard drive, examining the properties of individual files, and probing the drive's unallocated `slack space' to reveal deleted files." *Id.* at 547 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 540 (2005)). The government argued that under *Ickes*, the forensic searches were routine border searches, and therefore not subject to a reasonable suspicion requirement. *Id.* at 544, 546. But the court in *Saboonchi* distinguished *Ickes* on the ground that *Ickes* involved a manual digital search, whereas the search at issue in *Saboonchi* was a forensic digital search. *Id.* at 546. Thus, the district court in *Saboonchi* concluded that the holding of *Ickes* was limited to manual digital border searches of electronic devices, and hence did not apply to significantly more intrusive forensic digital searches. *Id.* at 569. Most significantly, the court in *Saboonchi* ultimately held that forensic digital searches are non-routine border searches, and therefore reasonable suspicion is required, because "[i]t is difficult to conceive of a property search more invasive or intrusive than a forensic computer search - it essentially is a body cavity search of a computer." *Id.* at 569. Importantly, however, unlike the search in *Ickes*, which was conducted by accessing the content of defendant's iPhone in the same manner as a typical user, the search of the Plaintiff's phone involved the copying of the entire data contained on the phone for subsequent examination and dissemination to other government agencies. Thus, the search of Plaintiff's Phone conducted at the airport was a non-routine border search that required some level of individualized suspicion. Therefore, *Ickes* does not dictate the outcome this case as the search of Plaintiff's Phone is clearly a non-routine border search.

VI. Dismissal as to the Non-DHS Defendants is Premature

As Plaintiff First Amended Complaint clearly shows, Plaintiff seeks, among other forms of relief, an injunction requiring the Defendants to reveal to whom they disclosed or disseminated information contained on his electronic device, (First Amended Compl., Prayer for Relief, C), and an injunction requiring the Defendants, including the "non-DHS" Defendants, to return all information obtained from his electronic device and if the information cannot be returned, to expunge or otherwise destroy it. (First Amended Compl., Prayer for Relief, B). In his Complaint, the Plaintiff has pleaded facts to support the requested reliefs. More specifically, the Plaintiff has pleaded facts pertaining to the four "non-DHS" Defendants including but not limited to the fact that Plaintiff has every reason to believe that the information obtained from his cell phone has been disclosed or disseminated to other agencies, organizations, individuals, or foreign governments, including but not limited to the other four non-DHS Defendants. The Defendants have not denied this claim or disputed Plaintiff's allegations. Instead, the defendants have only claimed that the claims against the other four non-DHS Defendants be dismissed because they are not involved in the wrongdoing against the Plaintiff. Considering that the DHS has not denied that the information obtained from Plaintiff's cell phone has been disclosed or disseminated to other agencies, organizations, individuals, or foreign governments, including but not limited to the other four non-DHS Defendants, dismissal of Plaintiff's claims against the non-DHS Defendants at this stage of the proceeding is clearly premature.

5. CONCLUSION

For the foregoing reasons, Plaintiff respectfully submits that the Court should deny the Defendants' motion to dismiss in its entirety.

Respectfully submitted by:

By: ***/S/George Anibowei***
George Anibowei
Texas Bar No. 24036142
The Law Office of George Anibowei, P.C.
6060 N. Central Expressway, Ste. 560
Dallas, Texas 75206
Telephone No: (214) 800-3463
Facsimile No: (214) 800-3464
Email: ganibowe@yahoo.com
ATTORNEY FOR PLAINTIFF, GEORGE ANIBOWEI

Dated this 1st day of May, 2017

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS

CERTIFICATE OF SERVICE (CM/ECF)

The undersigned hereby certifies that on May 1, 2017, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Northern District of Texas, using the electronic case filing system of the court. I also certify that a copy of this document was served on all parties via the Court's electronic filing system

Respectfully submitted,

By: ***/S/George Anibowei***
George Anibowei
Texas Bar No. 24036142
The Law Office of George Anibowei, P.C.
6060 N. Central Expressway, Ste. 560
Dallas, Texas 75206
Telephone No: (214) 800-3463
Facsimile No: (214) 800-3464
Email: ganibowe@yahoo.com
ATTORNEY FOR PLAINTIFF,
GEORGE ANIBOWEI